Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (previously presented) A method of distributing certificates to a plurality of mobile devices capable of communicating directly with each other comprising:
- attempting to establish a mobile ad hoc network (MANET) between said plurality of mobile devices at periodic predetermined times; and
- if said MANET can be established such that at least one of said plurality of mobile devices in said MANET is capable of obtaining certificates, distributing a certificate through said MANET to one or more of said plurality of mobile devices.

2. (previously presented) The method of claim 1 wherein a time period for which said certificate is valid is correlated to said periodic predetermined times.

3. (previously presented) The method of claim 1 wherein if one of said plurality of mobile devices is unable to retrieve a corresponding certificate within a preset time after said MANET is established, said one of said plurality of mobile devices subsequently attempts to participate in another ad-hoc network prior to a next predetermined time to retrieve said corresponding certificate.

4. (previously presented) The method of claim 1 wherein if one of said plurality of mobile devices is unable to retrieve a corresponding certificate within a present time after said MANET is established, said one of said plurality of mobile devices initiates a packet data call to obtain said corresponding certificate.

5. (previously presented) The method of claim 1 wherein an entity tracks which of said plurality of mobile devices have received currently valid certificates.

6. (previously presented) The method of claim 5 wherein corresponding certificates of said plurality of mobile devices which have not received an up-to-date certificate are distributed to another one of said plurality of mobile devices that communicates with said entity.

7. (previously presented) The method of claim 1 wherein said predetermined times are determined dynamically based upon measurements of times at which said plurality of mobile devices encounter each other.

8. (previously presented) The method of claim 1 wherein said certificate comprises a subset of full certificate information and said subset includes changed timing information and a signature.

9. (previously presented) A method of distributing certificates in a mobile ad-hoc network (MANET), said MANET having an access point for connecting to a communication network and comprising a plurality of mobile devices to be connected to said communication network through said access point, said method comprising
- retrieving at said access point, a plurality of certificates associated with respective ones of said plurality of mobile devices;
- storing said plurality of certificates at said access point; and
- upon establishing said MANET, forwarding said certificates through said MANET to said respective ones of said plurality of mobile devices.

10. (previously presented) The method of claim 9 wherein said access point queries those of said plurality of mobile devices with which it can exchange packets to determine an embedded root key.

11. (previously presented) The method of claim 10 wherein the access point obtains said plurality of certificates based upon said embedded root key.

12. (currently amended) [[A]] The method of ~~distributing certificates within a mobile ad-hoc network (MANET) of a plurality of mobile devices comprising having~~ claim 9 wherein an online entity is associated with at least one of said plurality of mobile devices to be responsible for both

distributing a certificate of said at least one of said plurality of mobile devices within said MANET and for obtaining other certificates needed to allow validation by corresponding others of said plurality of mobile devices in said MANET.

13. (previously presented) The method of claim 12 wherein said at least one of said plurality of devices is responsible for collecting embedded root keys of said others of said plurality of devices upon coming into contact therewith.

14. (original) The method of claim 13 wherein said root keys are reported to the online entity.

15. (previously presented) The method of claim 14 wherein said online entity returns other certificates to said at least one of said plurality of devices based upon reported root keys.

16. (previously presented) A method of securely setting a time source in a first mobile device capable of communicating with a second mobile device, said method comprising said first mobile device:
- establishing a shared secret with said second device using certificates;
- storing said shared secret in a non-volatile memory;
- authenticating said second device using said shared secret; and
- obtaining a time from said second device to enable said time source to be set.

17. (previously presented) The method of claim 16 wherein said shared secret is destroyed after an expiration time.

18. (previously presented) The method of claim 16 wherein said first device subsequently sets a clock via a secure time source upon establishing a connection thereto.

19. (previously presented) A method of a first mobile device validating a second mobile device, wherein said first and second mobile devices are capable of communicating with each other, said method comprising:
- said first mobile device obtaining a certificate from said second device;

- said first mobile device determining if said certificate has expired;
- if said certificate has not expired, said first mobile device using said certificate to validate said second mobile device; and
- if said certificate has expired, said first mobile device obtaining another certificate for said second mobile device using a pointer provided by said second mobile device and validating said second mobile device using said another certificate.

20. (previously presented) A method of distributing certificates when a first mobile device is unable to retrieve a certificate at a first time due to a lack of connectivity to a network, said method comprising:
- if said certificate has not been obtained by a second time, said first mobile device requesting assistance of other devices;
- having a second device from said other devices which has connectivity to said network request said certificate on behalf of said first device;
- upon obtaining said certificate, said second device reestablishing communication with said first device; and
- said second device sending said certificate to said first device.